

Clase 10 – Delitos informáticos, ciberseguridad y evidencia digital

Propósito y resultados de aprendizaje

La pregunta central no es cuántos delitos pueden memorizar, sino cómo reconocer límites jurídicos cuando desarrollan software, encuentran una vulnerabilidad o responden a un incidente.

Al terminar, deberían poder:

- Distinguir posibilidad técnica, autorización y legitimidad jurídica.
- Diferenciar un incidente, un incumplimiento y una conducta posiblemente delictiva, sin atribuir delitos automáticamente.
- Identificar los elementos básicos del acceso ilegítimo, el fraude y el daño informático.
- Delimitar una prueba de seguridad autorizada.
- Proponer una respuesta que proteja a las personas, reduzca el daño y preserve información útil.
- Explicar qué puede probar un log, una captura o un hash y qué no.

Esta clase continúa la protección de datos de la Clase 9 y retoma la forma y prueba digital de la Clase 4. No es un curso de explotación de vulnerabilidades ni de peritaje forense.

1. Apertura – «La aplicación me lo permitió»

La clase pasada vimos que detrás de una base de datos hay personas y derechos. Hoy vamos a agregar una dificultad: ustedes pueden tener conocimientos o permisos técnicos que les permitan hacer algo que jurídicamente no están autorizados a hacer.

Un sistema puede estar mal configurado. Una cuenta puede conservar permisos de más. Una aplicación puede mostrar información ajena. Nada de eso resuelve, por sí solo, si podemos seguir accediendo, copiar los datos o compartirlos.

Tampoco vamos a partir de la idea de que toda falla es un delito. Vamos a separar hechos, permisos, intención, consecuencias y prueba.

Caso conductor ficticio: TurnoApp

Una clínica contrata a una software factory para mantener TurnoApp. Alex integra el equipo de desarrollo y tiene autorización para trabajar en el entorno de pruebas con datos ficticios.

Mientras revisa un ticket, abre un enlace de producción que le compartieron y aparece una ficha médica ajena a la cuenta con la que ingresó. No había buscado esa ficha. Advierte que podría existir una falla de control de acceso.

En el chat del equipo aparecen cuatro propuestas:

- «Probemos con otras cuentas para ver cuántas historias clínicas se pueden consultar».
- «Descarguemos una muestra grande para que la clínica no pueda negar el problema».
- «Publiquemos capturas tapando los nombres».
- «Frenemos las consultas y avisemos por el canal de incidentes, conservando lo mínimo que ya tenemos».

Preguntas iniciales

1. ¿Es lo mismo encontrar la ficha sin buscarla que seguir consultando otras?
2. ¿Tener una cuenta de desarrollo autoriza a revisar datos de producción?
3. ¿Avisar después convierte en autorizado lo que se hizo antes?
4. ¿Qué harían durante los primeros cinco minutos?

Recoger respuestas sin anticipar una sentencia penal. Anotar en el pizarrón:
autorización — conducta — conocimiento — daño — evidencia.

2. Conceptos y acceso ilegítimo

Del problema técnico al problema jurídico

Antes de ponerle un nombre penal a lo que pasó, tenemos que describirlo bien.

Decir «hackearon la aplicación» puede parecer una explicación, pero suele mezclar preguntas distintas: ¿había una falla?, ¿alguien la aprovechó?, ¿se consultó información?, ¿se modificaron datos?, ¿se interrumpió el servicio?, ¿quién estaba autorizado a hacer qué?

En Derecho, esas diferencias no son detalles. Pueden cambiar el tipo de responsabilidad, las medidas necesarias y la prueba que necesitamos conservar.

En programación están acostumbrados a buscar la causa de un error. Acá vamos a hacer algo parecido: no empezar por la etiqueta, sino por los hechos.

Vulnerabilidad: una debilidad no es todavía un ataque

Una **vulnerabilidad** es una debilidad que puede comprometer la seguridad de un sistema.

Puede estar en el código, en una configuración, en la gestión de permisos o en la organización del trabajo. Por ejemplo, una aplicación permite que una cuenta de recepción vea información reservada al personal médico.

La debilidad existe aunque nadie la haya aprovechado. Por eso, encontrar una vulnerabilidad no permite afirmar automáticamente que hubo robo de datos ni identificar a una persona responsable de un ataque.

También hay una diferencia entre **autenticación** y **autorización**:

- La autenticación busca comprobar quién accede: por ejemplo, mediante una cuenta y un mecanismo de verificación.
- La autorización determina qué puede hacer esa cuenta: qué datos consultar, qué funciones ejecutar y en qué entorno.

Una aplicación puede autenticar correctamente a una persona y, sin embargo, permitirle operaciones que no le corresponden.

Ejemplo: el sistema reconoce correctamente a Alex, pero le muestra la ficha de un paciente que no debería poder consultar. El problema no necesariamente está en el inicio de sesión; puede estar en el control de acceso a esa información.

Pregunta para el grupo: ¿que el servidor responda a una solicitud demuestra que la persona tenía derecho a recibir esos datos?

La respuesta es no: demuestra una respuesta técnica. Su legitimidad requiere otro análisis.

Incidente de seguridad: qué se comprometió

Un **incidente de seguridad** es un evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de información o sistemas.

Esas tres palabras tienen consecuencias concretas:

- **Confidencialidad:** que la información no quede accesible a personas no autorizadas. Ejemplo: una ficha médica aparece en una cuenta ajena.
- **Integridad:** que los datos no sean alterados indebidamente. Ejemplo: alguien modifica una indicación o un resultado sin autorización.
- **Disponibilidad:** que la información y el servicio estén accesibles para quienes deben utilizarlos cuando los necesitan. Ejemplo: una interrupción impide consultar las indicaciones de un paciente.

Un incidente puede afectar una, dos o las tres dimensiones. Puede originarse en un ataque, pero también en un error de configuración, una falla de infraestructura o una operación accidental.

En TurnoApp, la visualización de la ficha permite advertir una exposición de información. Todavía no prueba que se hayan alterado las historias clínicas ni que la base completa haya sido descargada.

Idea para explicar oralmente: «No saber todavía cuánto pasó no significa que no haya que actuar. Significa que debemos actuar sin presentar como comprobado lo que aún estamos investigando».

Incumplimiento contractual: qué se había prometido

Un **incumplimiento contractual** es el apartamiento de una obligación asumida.

Si la software factory se comprometió a implementar permisos diferenciados, revisar determinadas configuraciones o responder a incidentes por un canal acordado, hay que comparar lo ocurrido con esas obligaciones.

No alcanza con decir «el sistema falló». Debemos preguntar qué se contrató, quién tenía a cargo cada tarea y qué actuación concreta se reprocha.

Ejemplo: el contrato exigía separar el entorno de pruebas del de producción y esa separación no se implementó. Puede existir una cuestión contractual aunque no haya evidencia de un ataque.

Tampoco toda vulnerabilidad demuestra por sí sola un incumplimiento indemnizable. Hay que examinar el contrato y los presupuestos de la responsabilidad correspondiente; no presumir que cualquier resultado adverso prueba automáticamente la responsabilidad del equipo.

Infracción en protección de datos: deberes aunque no aparezca un atacante

Una **infracción en protección de datos** supone el incumplimiento de obligaciones aplicables al tratamiento.

La Ley 25.326 exige medidas de seguridad y confidencialidad. Por eso, una organización no puede cerrar el análisis diciendo «no sabemos quién entró». También debe revisar cómo protegía los datos, quién tenía permisos y qué hizo al conocer el problema.

Ejemplo: usar historias clínicas reales en un ambiente de pruebas accesible a todo el equipo puede plantear problemas de tratamiento, seguridad y confidencialidad aunque ninguna persona las haya vendido o publicado.

La evaluación no se agota en si hubo un delito. Los datos personales merecen protección antes de que exista una condena penal.

Delito: por qué no basta con que algo esté mal

Para afirmar responsabilidad penal no alcanza con una conducta inconveniente, un daño o la infracción de una regla interna. Deben acreditarse los requisitos del delito correspondiente.

Como esquema inicial, sin agotar la teoría del delito, necesitamos preguntar:

1. **¿La conducta encuadra en una descripción penal?** Es la pregunta por la tipicidad.
2. **¿Existe alguna causa que justifique jurídicamente esa conducta?** No basta con alegar una buena intención.
3. **¿Puede atribuirse responsabilidad personal en las condiciones del caso?** No se deduce solo del puesto, del conocimiento técnico o del resultado.

Los planos contractual, administrativo, civil y penal pueden coexistir, pero no se reemplazan entre sí. Una multa administrativa no demuestra por sí sola un delito; la ausencia de condena penal tampoco elimina automáticamente las demás responsabilidades.

Legalidad, tipicidad y dolo, explicados desde programación

Legalidad: no se puede crear un delito por semejanza o porque una conducta nos parezca peligrosa. La exigencia de ley penal previa se vincula con el art. 18 de la Constitución Nacional.

Tipicidad: los hechos deben reunir los elementos de la figura legal. Una etiqueta como «hackeo» no sustituye esa comprobación.

Podemos compararlo, con límites, con verificar condiciones de una regla: no alcanza con que una condición se cumpla si faltan otras que también exige. La diferencia es que el Derecho requiere interpretar hechos, conceptos y prueba; no funciona como una comprobación automática de código.

Dolo: en una primera aproximación, supone conocimiento y voluntad de realizar la conducta típica. No equivale necesariamente a querer enriquecerse, destruir información o perjudicar personalmente a alguien.

En el acceso ilegítimo, decir «solo quería mirar» no resuelve el problema si se sabía que se estaba accediendo sin autorización a información restringida.

Por el contrario, una aparición inesperada de información no debe equipararse automáticamente a una búsqueda deliberada. Hay que distinguir lo accidental de las decisiones tomadas una vez advertida la situación.

Ejemplo de contraste: recibir por error una ficha ajena y cerrar la consulta no es lo mismo que advertir la falla y continuar accediendo a más fichas. No anunciamos una condena en ninguna escena: identificamos hechos que cambian el análisis.

Artículo 153 bis del Código Penal: lectura completa

Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

La Ley 26.388 incorporó esta figura al Código Penal. Para aplicarla debemos leer cada elemento, no quedarnos con la expresión «acceso ilegítimo».

a) «Accediere por cualquier medio»

La norma no exige un método sofisticado ni que la persona sepa programar. Puede discutirse el acceso realizado con credenciales ajenas, con permisos indebidamente conservados o aprovechando una falla.

Pero conocer una dirección, observar que existe un servicio o advertir una vulnerabilidad no equivale necesariamente a haber accedido al sistema o dato restringido. Hay que precisar qué operación ocurrió y a qué información o función se llegó.

b) «A un sistema o dato informático de acceso restringido»

La restricción es un elemento que debe comprobarse. No todo lo que está en internet es público, ni todo sitio accesible contiene únicamente información de libre consulta.

Una página puede ser pública y alojar funciones o datos reservados. También puede haber material genuinamente abierto al público cuyo acceso no encuadre en esta figura.

Ejemplo: el horario de atención publicado por una clínica no se equipara a las fichas médicas almacenadas detrás de sus funciones de gestión.

La ausencia de una barrera técnica eficaz no demuestra, por sí sola, ni la autorización ni la configuración del delito. Deben analizarse la naturaleza de la información, las restricciones existentes y los demás elementos del caso.

c) «Sin la debida autorización o excediendo la que posea»

La autorización no es necesariamente un «sí» o un «no» para todo el sistema. Puede estar delimitada por:

- **Activo:** una aplicación, no todos los servicios de la organización.
- **Entorno:** pruebas, no producción.
- **Función:** diagnosticar una falla, no consultar información personal sin necesidad.
- **Tiempo:** mientras dura una intervención o un vínculo.
- **Datos:** información ficticia o un conjunto expresamente habilitado.
- **Operación:** lectura, modificación, exportación u otra actuación autorizada.

Ejemplo: una persona deja de trabajar para una empresa y su cuenta sigue activa. La falla en la revocación de permisos no significa que conserve autorización para entrar.

También importa quién puede autorizar. El permiso de una persona sin facultades sobre el sistema o los datos no resuelve automáticamente la legitimidad del acceso.

d) «A sabiendas»

Debe analizarse el conocimiento de las circunstancias relevantes del acceso. No se presume únicamente por ser parte del equipo de sistemas.

Pueden resultar relevantes el alcance informado de la tarea, las advertencias recibidas, las comunicaciones y la conducta antes y después del hallazgo. Ningún indicio aislado reemplaza la valoración del conjunto.

Avisar después puede ser relevante para comprender lo ocurrido, pero no crea retroactivamente una autorización que no existía.

e) «Si no resultare un delito más severamente penado»

Es una cláusula de subsidiariedad expresa. Advierte que el acceso puede integrar un episodio alcanzado por una figura más grave y que no corresponde sumar mecánicamente penas por cada etiqueta disponible.

Para los estudiantes, la consecuencia práctica es simple: describir con precisión el acceso y lo que sucedió después. La calificación final requiere un análisis jurídico completo.

f) La agravante del segundo párrafo

La norma distingue ciertos sistemas o datos estatales, de proveedores de servicios públicos y de servicios financieros. Hay que verificar la condición y el perjuicio exigidos, no deducir la agravante del diseño de una página, su popularidad o la sola presencia de un logotipo.

Tampoco debe trasladarse esta agravante a cualquier aplicación de salud: el art. 184 contempla supuestos propios de daño agravado que se estudian en el bloque siguiente.

TurnoApp: analizar la secuencia, no juzgar a Alex por una etiqueta

Primer momento: la tarea asignada. Alex está autorizado a trabajar con datos ficticios en pruebas. Ese es el punto de partida, no una habilitación general sobre producción.

Segundo momento: aparece la ficha ajena. Debemos averiguar cómo llegó el enlace, qué hizo Alex, qué mostraba la pantalla y cuándo advirtió la situación. No convertir el hallazgo inesperado en una intrusión deliberada por presunción.

Tercer momento: ya reconoce el problema. Ahora debe decidir si se detiene y comunica o si continúa explorando. Esa decisión agrega hechos nuevos al análisis.

Cuarto momento: eventual copia o difusión. Descargar fichas o compartir capturas puede generar problemas adicionales de privacidad, confidencialidad y tratamiento. No son consecuencias necesarias del hallazgo y no se justifican automáticamente por querer demostrarlo.

Conclusión para explicar: «No evaluamos si Alex es “hacker” o “buena persona”. Evaluamos qué hizo, qué sabía, qué tenía permitido y qué se puede probar».

Bancos de datos y comunicaciones: por qué no todo se analiza con el mismo artículo

Art. 157 bis CP — bancos de datos personales. Contempla el acceso a sabiendas e ilegítimo —o violando sistemas de confidencialidad y seguridad de datos— a bancos de datos personales; también determinadas revelaciones e inserciones ilegítimas.

La revelación prevista en el inciso 2 exige atender, entre otros elementos, al deber de preservar el secreto por disposición legal. No toda comunicación de cualquier dato reúne automáticamente esa figura.

En TurnoApp, una base de historias clínicas exige considerar esta norma y la Ley 25.326. Que sea técnicamente una base de datos no basta: importan la información personal contenida y la conducta concreta.

Art. 153 CP — comunicaciones. Comprende supuestos de acceso indebido a comunicaciones no dirigidas a quien accede e interceptación o captación indebida, entre otras conductas.

Ejemplo: administrar el servidor de correo no equivale a tener permiso general para leer los mensajes personales de quienes lo utilizan. La disponibilidad de una herramienta administrativa no reemplaza la justificación jurídica de su uso.

La relación entre estas figuras y el art. 153 bis debe resolverse en cada caso. No corresponde asumir tres delitos independientes por el solo hecho de que intervengan un sistema, datos y mensajes.

Preguntas breves para comprobar comprensión

1. «No descargué nada, solo leí». ¿Descarta el art. 153 bis?

No necesariamente. La figura se centra en el acceso con los requisitos legales; no exige en su descripción básica una descarga masiva o una venta posterior.

2. «Usé mi propia cuenta». ¿Demuestra autorización?

No. Hay que revisar qué facultades tenía esa cuenta y qué podía hacer jurídicamente su titular.

3. «La empresa protegió mal los datos». ¿Eso habilita a revisarlos?

No. La eventual responsabilidad de la organización no concede por sí sola autorización a terceros.

4. «Incumplió los términos de uso». ¿Eso demuestra un delito?

Tampoco. Los términos pueden aportar contexto, pero la responsabilidad penal exige comprobar los elementos de una figura legal.

Síntesis del bloque: posibilidad técnica no equivale a permiso; permiso no equivale a autorización ilimitada; y una conducta cuestionable no equivale automáticamente a delito.

- Apoyo docente — cómo administrar la ampliación en 20 minutos
 - 5 minutos: vulnerabilidad, incidente y planos de responsabilidad; usar los ejemplos de TurnoApp en vez de leer todas las definiciones.
 - 3 minutos: legalidad, tipicidad y dolo.
 - 8 minutos: lectura del art. 153 bis y análisis de autorización, restricción y conocimiento; integrar en este momento la secuencia de Alex.
 - 2 minutos: diferencia con bancos de datos y comunicaciones.
 - 2 minutos: elegir dos preguntas de comprensión y cerrar con la síntesis.
- El texto desarrollado funciona como apunte y apoyo para explicar, no como un guion que deba leerse íntegramente. Si aparece una discusión extensa, reservar las preguntas restantes para el taller sin quitarle su tiempo.

3. Fraude, daño y otras conductas

Phishing y fraude: describir antes de calificar

Phishing: técnica de engaño que busca obtener información, credenciales o inducir acciones aparentando una identidad o comunicación confiable. Es una descripción del mecanismo, no una calificación penal única.

Comparar dos escenas:

Escena A. Un mensaje falso convence a una persona de transferir dinero a una supuesta cuenta de soporte. Hay que analizar la estafa del art. 172 CP: engaño, error, disposición patrimonial y perjuicio, según las circunstancias.

Escena B. Una manipulación informática altera operaciones o la transmisión de datos y produce una defraudación. Corresponde examinar el art. 173 inc. 16 CP:

El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Distinción esencial: no todo fraude realizado por internet encuadra automáticamente en el inciso 16. Importa cómo se produjo la disposición o afectación patrimonial. Un mismo episodio puede comprender varias etapas y requerir examinar otras figuras.

Pregunta: «¿La víctima transfirió engañada, se alteró una operación del sistema o sucedieron ambas cosas? ¿Qué información falta?».

Daño informático — arts. 183 y 184 CP

El segundo párrafo del art. 183 contempla alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos; también las conductas allí previstas respecto de programas destinados a causar daños.

Ejemplos para discutir:

- Una persona que dejó la empresa borra deliberadamente la base de producción.
- Un despliegue defectuoso elimina registros por un error no intencional.
- Se distribuye un programa destinado a causar daños.
- Un equipo restaura un backup autorizado como parte de una recuperación documentada.

No son situaciones equivalentes. En cada una se revisan conducta, autorización, conocimiento, finalidad y efectos. Un bug no se convierte automáticamente en daño penal.

El art. 184 prevé agravantes; los incisos 5 y 6 incluyen determinados datos o sistemas públicos y sistemas destinados a servicios de salud, comunicaciones y otros servicios públicos. Una app de salud exige atender especialmente a la función concreta del sistema, sin presumir todos los requisitos por su nombre comercial.

Ransomware

Es una modalidad de ataque que puede impedir el acceso a información y acompañarse de una exigencia de pago o amenaza de divulgación. No es el nombre de un único artículo del Código Penal.

Según los hechos, pueden examinarse acceso ilegítimo, daño, extorsión del art. 168 y otras figuras. No toda infección tiene idéntica calificación ni deben sumarse delitos sin analizar su relación.

Para un equipo de programación, la prioridad no es resolver en soledad ese concurso jurídico, sino activar respuesta, reducir riesgos y documentar hechos útiles para especialistas y autoridades.

Suplantación, hostigamiento y grooming: evitar etiquetas automáticas

- Una cuenta falsa no acredita por sí sola un delito autónomo y general de «suplantación» en el Código Penal nacional. Debe examinarse qué se hizo: engaño patrimonial, amenazas, acceso a cuentas, difusión de información u otra conducta, y las normas locales que correspondan.
- «Ciberacoso» describe situaciones diversas. No toda interacción ofensiva tiene la misma respuesta penal.
- El **art. 131 CP** contempla el contacto tecnológico con una persona menor de edad con el propósito de cometer un delito contra su integridad sexual. No debe confundirse con cualquier hostigamiento online.

Estas distinciones no minimizan el daño: evitan que la gravedad social de un hecho sustituya el análisis jurídico.

4. Seguridad autorizada y ejercicio profesional

Definiciones útiles

Ciberseguridad defensiva: medidas para prevenir, detectar, contener y recuperar frente a riesgos e incidentes.

Prueba de penetración: evaluación de seguridad que puede emplear técnicas de ataque en un alcance previamente acordado. Las técnicas no se vuelven lícitas solo porque quien las usa se denomine «hacker ético».

Una finalidad de seguridad es relevante, pero no constituye por sí sola un permiso general para ingresar a sistemas ajenos. Las posibles causas de justificación requieren presupuestos específicos; no se presumen por una buena intención.

Qué debe delimitar una autorización profesional

Antes de probar, dejar documentado:

- Quién autoriza y si tiene facultades sobre los sistemas y datos involucrados.
- Qué activos y ambientes comprende: pruebas no equivale a producción.
- Qué técnicas y operaciones están permitidas y cuáles prohibidas.
- Ventana temporal, responsables y canal de contacto.
- Tratamiento de información personal, confidencial y de terceros.
- Límites de carga, continuidad y condiciones para detenerse.
- Gestión de hallazgos, conservación y devolución o eliminación acordada de material.

- Coordinación con proveedores externos cuando sus servicios puedan verse afectados.

La forma escrita ayuda a acreditar alcance; no es una garantía absoluta de impunidad ni habilita a quien autoriza a disponer de derechos ajenos que no controla.

Tres comparaciones rápidas

Repositorio público. Una clave expuesta no concede autorización para usarla. La respuesta responsable es reportar por un canal adecuado, no comprobar qué datos permite extraer.

Programa de recompensas. Deben leerse las reglas: activos incluidos, exclusiones, límites y procedimiento de reporte. La existencia de una recompensa no autoriza cualquier prueba.

Pedido informal. «Fijate si es seguro» puede ser insuficiente para delimitar una intervención riesgosa. Precisar alcance antes de actuar.

Confidencialidad y deber de seguridad

Los arts. 9 y 10 de la Ley 25.326 conectan seguridad técnica con obligaciones jurídicas. El art. 9 exige medidas técnicas y organizativas necesarias; el art. 10 impone confidencialidad a quienes intervienen en el tratamiento, incluso después de finalizado el vínculo.

En TurnoApp, no corresponde usar información médica real para pruebas o demostraciones innecesarias. Tapar un nombre no garantiza anonimización: otros datos pueden permitir identificar a la persona.

5. Qué hacer ante el incidente y qué conservar

Primeras decisiones

1. **Detener la exploración no autorizada.** No ampliar el acceso para medir el problema por cuenta propia.
2. **Activar el canal de incidentes.** Informar al responsable previsto, con datos mínimos y comunicación restringida.
3. **Contener el riesgo con autorización y criterio técnico.** La protección de pacientes y servicios tiene prioridad; no mantener una exposición activa solo para observarla.
4. **Preservar lo disponible de manera lícita.** Evitar borrados, reinstalaciones o cambios improvisados y registrar las acciones necesarias.
5. **Escalar a seguridad, asesoramiento jurídico y autoridad competente cuando corresponda.** No atribuir públicamente autoría ni anunciar un diagnóstico no verificado.

No hay una receta universal de «apagar todo» o «no tocar nada». El aislamiento, la captura de información volátil o la recuperación dependen de especialistas y del contexto. Una contención urgente puede modificar evidencia: debe justificarse y documentarse.

Conceptos de evidencia

Evidencia digital: información almacenada o transmitida digitalmente que puede contribuir a esclarecer hechos. Su utilidad depende de su procedencia, integridad, contexto y obtención legítima.

Integridad: posibilidad de comprobar que el material no fue alterado respecto de un punto de referencia confiable.

Autenticidad: vinculación del material con la fuente o hecho que se afirma que representa.

Cadena de custodia: registro documentado del manejo de elementos: quién los obtuvo, cuándo, cómo, dónde se resguardaron, quién accedió y qué transferencias o intervenciones tuvieron. Un archivo subido a una carpeta no constituye por sí solo una cadena de custodia.

Lo que un hash prueba y lo que no

Una función hash produce una huella digital a partir de los datos. Comparar hashes con un algoritmo adecuado, como SHA-256, permite controlar coincidencia de contenido y detectar modificaciones respecto del registro inicial.

No prueba, por sí solo:

- Quién creó el archivo o realizó la acción.
- Que el contenido fuera verdadero antes de calcularlo.
- Que la fecha declarada sea auténtica.
- Que la obtención haya sido lícita.

Un archivo manipulado antes de su primer hash seguirá teniendo un hash calculable. La huella no corrige la falta de procedencia.

Capturas, logs e IP

Captura: puede ser útil para mostrar lo observado, pero necesita contexto y corroboración. No reemplaza automáticamente al archivo o registro original. No difundir datos sensibles para conseguir una «mejor prueba».

Log: puede registrar eventos, cuenta utilizada, fechas y otros datos. Hay que conocer el sistema que lo generó, permisos de modificación, zona horaria y sincronización de reloj. Un log incompleto o alterable exige cautela.

IP: es un dato de conexión, no una identidad humana incontrovertible. Pueden intervenir cuentas compartidas, redes comunes, intermediarios o credenciales comprometidas. Atribuir una acción requiere correlación y prueba adicional.

Registro mínimo del hallazgo

Conservar por canal seguro, sin ampliar el acceso:

- Fecha, hora y zona horaria de la observación.
- Entorno y cuenta propia utilizada, sin copiar contraseñas ni tokens al informe.
- Qué se observó y qué acción previa lo produjo.
- Alcance conocido y alcance todavía desconocido.
- Material ya disponible y procedencia.
- Personas notificadas y acciones ejecutadas con su horario.

Separar el original restringido de la copia de trabajo redactada o anonimizada. Registrar esa transformación; no sobrescribir el original para ocultar datos en una copia destinada a circular.

Preservación no es entrega de información

La guía UFECI-DIGCRI de 2020 distingue el resguardo de datos almacenados por proveedores de su posterior obtención. Evitar su pérdida no equivale a poder leerlos ni recibirlos sin las vías correspondientes.

Sus procedimientos para autoridades no convierten a un desarrollador en investigador autorizado. Tampoco corresponde trasladar mecánicamente a todos los proveedores los plazos descritos en esa guía histórica.

UFECI: unidad especializada del Ministerio Público Fiscal de la Nación.
UFEDyCI: unidad especializada del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. No son el mismo organismo ni una fiscalía

universal para todos los hechos ocurridos en internet. La intervención se define según competencia y jurisdicción; en provincia de Buenos Aires debe canalizarse ante las autoridades competentes de esa jurisdicción cuando corresponda.

6. Doctrina y jurisprudencia para pensar

Doctrina: leer el límite, no solo el nombre del delito

Ricardo Gutiérrez, Laura C. Radesca y Marcelo A. Riquert, en su comentario al art. 153 bis publicado en el Código Penal comentado de Pensamiento Penal, examinan el acceso restringido, la autorización y sus excesos, y discuten la intervención penal y los supuestos vinculados con seguridad informática.

Para la clase, trabajar sus apartados «Tipo objetivo», «Verbo típico» y «Casos de atipicidad» —páginas 6 a 11 del PDF—, sin presentar sus posiciones como unanimidad doctrinaria.

El texto también contiene referencias históricas de derecho comparado que no deben tratarse como descripción vigente de otros países. Algunas posiciones sobre pruebas de seguridad son discutibles: no deben transformarse en la consigna «si quiero mejorar la seguridad, puedo entrar».

Pregunta: ¿por qué el Derecho exige discutir el alcance del permiso en lugar de decidir solo si alguien se considera una buena persona?

Jurisprudencia: CSJN, «Quaranta, José Carlos s/ inf. ley 23.737», 31/08/2010, Q.124.XLI

Hechos relevantes: una intervención telefónica se ordenó sobre la base de información insuficiente proveniente de una denuncia anónima. De esa medida surgió la investigación que condujo a la condena.

Decisión de la mayoría: la Corte examinó la falta de fundamentación y de elementos objetivos para la intervención, declaró la nulidad de lo actuado y absolvió. Argibay disintió por inadmisibilidad del recurso, con remisión al art. 280 CPCCN.

Fundamento para trabajar: la intromisión estatal en comunicaciones requiere control judicial previo y fundamentado; el hallazgo posterior de información incriminante no subsana por sí solo la falta de justificación original. Leer considerandos 17 a 24.

Alcance preciso: es un precedente sobre intervención estatal de comunicaciones y prueba ilegítima, no una sentencia sobre TurnoApp, pruebas de penetración, hashes ni aplicación del art. 153 bis. Se usa como referencia constitucional para comprender límites de la obtención de prueba; no permite afirmar que toda irregularidad en una evidencia digital produzca automáticamente nulidad.

Aplicación pedagógica: si incluso la investigación estatal debe respetar garantías, «quiero demostrar la falla» no constituye una autorización general para investigar datos ajenos.

Texto íntegro del fallo leído en copia reproducida por Pensamiento Penal. No se presenta esa reproducción como una consulta directa a la base oficial de la Corte.

7. Taller — responder sin agravar el problema

Organización

- 3 minutos: lectura de la continuación del caso.
- 12 minutos: resolución en equipos.
- 8 minutos: puesta en común y contraste de decisiones.
- 2 minutos: devolución docente.

Continuación del caso ficticio

El equipo comunica el hallazgo de Alex a la clínica. Todavía no se conoce la cantidad de personas afectadas ni si hubo descargas anteriores.

Una persona del equipo propone reiniciar y actualizar todos los servidores inmediatamente. Otra quiere copiar la base a su nube personal para «tener un respaldo». Una tercera encontró en los logs una IP y afirma que ya identificó al responsable. El contrato permite mantenimiento, pero no detalla pruebas de seguridad sobre datos reales.

La clínica pide restablecer el servicio y averiguar qué pasó. No autoriza una difusión pública ni una extracción indiscriminada de historias clínicas.

Consigna para estudiantes

Entregar una hoja con:

1. Hechos comprobados, hipótesis y datos que faltan.
2. Tres conductas que deben detenerse o descartarse y su justificación.
3. Plan de cinco acciones ordenadas para responder al incidente.
4. Dos posibles cuestiones jurídicas, con artículos pertinentes y requisitos todavía no comprobados.
5. Evidencia a preservar: fuente, responsable o rol interviniente, resguardo y registro de accesos.
6. Una explicación de por qué una IP o un hash no resuelven por sí solos la autoría.
7. Mensaje interno de hasta seis líneas para informar el hallazgo sin exponer información médica ni afirmar un ataque no comprobado.

No se realizan accesos reales, descargas, escaneos ni pruebas contra servicios de terceros. Se trabaja exclusivamente sobre la descripción ficticia.

- Guía de resolución docente — no incluir en la consigna del campus

1. Hechos e incertidumbres

Se conoce la aparición de una ficha ajena en producción y el alcance inicial de la autorización de Alex. No está demostrada una extracción masiva, la identidad de un atacante, la extensión temporal, el total de afectados ni una acción deliberada de Alex durante el hallazgo inicial.

Una falla de control de acceso es una hipótesis técnica fundada que debe confirmarse por personal autorizado; no equivale a un ataque externo demostrado.

2. Conductas que no corresponden

- No consultar más fichas ni descargar una muestra masiva por cuenta propia: amplía la exposición y puede exceder la autorización.
- No copiar la base a una nube personal: agrega un destino y accesos no autorizados para información sensible.
- No publicar capturas ni señalar responsables por una IP: aumenta riesgos de privacidad y atribución errónea.
- El reinicio general no debe ejecutarse como reflejo: requiere valoración técnica, continuidad del servicio y registro de su impacto. Tampoco corresponde conservar un peligro activo solo para no alterar registros.

3. Secuencia de respuesta admisible

- Frenar accesos exploratorios y comunicar al canal designado con información mínima.

- Convocar al responsable de seguridad, a la clínica y a asesoramiento jurídico; definir facultades y alcance.
- Contener la exposición con medidas autorizadas, proporcionadas y documentadas, atendiendo a la continuidad asistencial.
- Resguardar registros y material disponible, antes de cambios destructivos cuando sea viable; registrar toda intervención necesaria.
- Investigar y recuperar por personal autorizado; evaluar comunicaciones, asistencia y denuncia ante autoridad competente según los hechos.
- Se admiten ajustes del orden si el equipo justifica una urgencia concreta. No exigir una secuencia rígida que mantenga el daño.

4. Análisis jurídico esperado

- Art. 153 bis: revisar acceso restringido, autorización y actuación a sabiendas; no imputar automáticamente el hallazgo fortuito.
- Art. 157 bis: examinar el acceso o revelación ilegítimos de información de un banco de datos personales.
- Ley 25.326, arts. 9 y 10: deber de seguridad y confidencialidad; el contrato de mantenimiento no habilita cualquier tratamiento.
- Arts. 183 y 184: pertinentes solo si aparecen hechos de alteración, destrucción o inutilización y los restantes requisitos; no atribuir daño penal por la mera falla.
- La defraudación requiere hechos patrimoniales y un mecanismo concreto; en esta continuación no está demostrada.
- No premiar la cantidad de delitos nombrados. Premiar la capacidad de explicar por qué una figura podría ser pertinente y qué falta para sostenerla.

5. Evidencia

Logs de la aplicación y autenticación, registro del ticket original, configuración y versiones relevantes, comunicaciones del reporte y acciones de contención. Su acceso y copia deben estar autorizados y limitados.

Registrar origen, horarios, zona horaria, método de obtención, personas que intervienen y ubicación de resguardo. Calcular hash de los archivos obtenidos lícitamente cuando corresponda, conservando el dato de cómo y cuándo se generó la copia. No transformar este ejercicio en una exigencia de imagen forense hecha por estudiantes.

6. IP y hash

La IP puede ayudar a correlacionar conexiones, pero no identifica por sí sola a la persona que actuó. El hash sirve para controlar integridad respecto de una referencia, no para demostrar autoría, veracidad o licitud.

7. Modelo de mensaje interno

Durante la revisión del ticket se visualizó en producción una ficha ajena a la cuenta utilizada. Se detuvo la consulta, sin ampliar el acceso. Se informa una posible exposición de datos de salud; todavía no se conoce su alcance ni se ha confirmado una extracción. Solicitamos activar el protocolo de incidentes y designar responsables para la contención y preservación de registros. El detalle mínimo queda disponible por el canal restringido.

Criterios de devolución

- Distingue hechos e hipótesis.
- Explica los límites de la autorización.
- Usa las normas sin conclusiones automáticas.
- Protege datos y continuidad del servicio.
- Propone evidencia pertinente con trazabilidad.
- Comunica con precisión y sin alarmismo.
- Es una actividad formativa. No se fija aquí una nueva condición de aprobación de los parciales.

8. Cierre

Texto de cierre oral

Programar profesionalmente no consiste solamente en lograr que el sistema funcione. También exige reconocer cuándo una acción requiere autorización, cuándo corresponde detenerse y cómo informar un problema sin agravarlo.

Hoy no buscamos que memoricen un listado de penas. Buscamos que puedan distinguir una falla de una conducta deliberada, un permiso técnico de una autorización y un dato llamativo de una prueba suficiente.

La capacidad técnica permite actuar. El criterio profesional ayuda a decidir cuándo corresponde hacerlo y con qué límites.

Salida individual

Responder en tres frases:

1. Encontrar una vulnerabilidad no me autoriza a...

2. Ante una exposición de datos, mi primera decisión responsable sería...
3. Un hash permite controlar..., pero no demuestra...

Apunte breve para estudiantes

- Vulnerabilidad, incidente, incumplimiento y delito no son sinónimos.
- La autorización debe cubrir la acción, el sistema, los datos y el momento.
- El art. 153 bis contempla acceder a sabiendas, sin autorización o excediéndola, a sistemas o datos de acceso restringido.
- El art. 157 bis exige atender especialmente al acceso y a otras conductas sobre bancos de datos personales.
- El phishing es un mecanismo: la figura penal depende de cómo ocurre el hecho.
- No todo error de software es daño penal ni todo ransomware corresponde a un único delito.
- Una finalidad «ética» no reemplaza la autorización para pruebas.
- Hay que contener el riesgo y documentar las intervenciones, sin investigar por cuenta propia.
- Capturas y logs requieren contexto; una IP no es una persona.
- El hash ayuda a controlar integridad, no certifica autoría ni licitud.
- Preservar información no equivale a tener derecho a acceder a ella.
- La obtención de prueba también debe respetar derechos.

Fuentes y lecturas

Normativa

- [Código Penal — texto actualizado, fuente oficial](#): arts. 131, 153, 153 bis, 157 bis, 168, 172, 173 inc. 16, 183 y 184.
- [Ley 26.388 — texto original oficial](#): antecedente de la reforma. Para vigencia, utilizar el Código actualizado, no presumir que todo artículo del texto original conserva su redacción.
- [Ley 25.326 — texto actualizado oficial](#): arts. 9 y 10. Continuidad con la Clase 9.

Doctrina

- Ricardo Gutiérrez, Laura C. Radesca y Marcelo A. Riquert, [«Violación de secretos y de la privacidad. Art. 153 bis»](#), Código Penal comentado, Pensamiento Penal. Apartados consultados: tipo objetivo, verbo típico y casos de atipicidad. Es una contribución doctrinaria con posiciones debatibles y referencias históricas, no una norma ni una descripción actual del derecho comparado.

Jurisprudencia

- CSJN, «Quaranta, José Carlos s/ inf. ley 23.737», 31/08/2010, Q.124.XLI. [Texto íntegro reproducido por Pensamiento Penal](#). Considerandos 17-24; disidencia de Argibay. Lectura constitucional sobre intervención de comunicaciones y exclusión probatoria, no precedente específico de acceso ilegítimo.

Guías y organismos

- UFEI-DIGCRI, [Guía de buenas prácticas para obtener evidencia electrónica en el extranjero, 2020](#), secciones I–III. Fuente para distinguir preservación y obtención; revisar requisitos actuales del proveedor en una gestión real.
- [UFEI – Ministerio Público Fiscal de la Nación](#).
- [Funciones y áreas de UFEI](#).
- [Fiscalías y unidades del Ministerio Público Fiscal de CABA](#): referencia institucional de UFEDyCI.